Strategy Research Project

A STRATEGIC APPROACH TO NETWORK DEFENSE: FRAMING THE CLOUD

BY

COLONEL TIMOTHY K. BUENNEMEYER
United States Army

USAWC CLASS OF 2011

U.S. Army War College, Carlisle Barracks, PA 17013-5050

The U.S. Army War College is accredited by the Commission on Higher Education of the Middle State Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
10-03-2011	Strategy Research Project	

4. TITLE AND SUBTITLE

A Strategic Approach to Network Defense: Framing the Cloud

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Colonel Timothy K. Buennemeyer

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Captain James D. Heffernan
Department of Command, Leadership, and Management

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

U.S. Army War College
122 Forbes Avenue
Carlisle, PA 17013

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Distribution A: Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

This paper examines current Internet attack trends in the computer networking environment and proposes an enhanced framework for system defense that is applicable to both corporate and government networks. Network defenses are typically designed, implemented, and managed at corporate computing centers and in the U.S. Department of Defense, at installation-level and regional area processing centers. Industry-wide Information Assurance best business practices and computer defensive measures are not uniformly implemented, so an enhanced security framework is necessary to assist with prioritizing and coordinating defensive efforts. The U.S. Chief Information Officer proposes that the Federal Government migrate its vast network of computer systems, through consolidation, to a more enterprise-focused architectural solution. This effort requires an expanded security framework, based on accepted network defensive principles, to reduce risks associated with emerging virtualization capabilities and scalability of cloud computing. This expanded defensive framework can assist enterprise networking and cloud computing architects to better design more secure systems.

15. SUBJECT TERMS

Network Security, Cloud Computing, Cyber

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. TELEPHONE NUMBER** *(include area code)*
UNCLASSIFED	UNCLASSIFED	UNCLASSIFED	UNLIMITED	34	

USAWC STRATEGY RESEARCH PROJECT

A STRATEGIC APPROACH TO NETWORK DEFENSE: FRAMING THE CLOUD

by

Colonel Timothy K. Buennemeyer
United States Army

Captain James D. Heffernan
Project Adviser

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR: Colonel Timothy K. Buennemeyer

TITLE: A Strategic Approach to Network Defense: Framing the Cloud

FORMAT: Strategy Research Project

DATE: 10 March 2011 WORD COUNT: 6,008 PAGES: 34

KEY TERMS: Network Security, Cloud Computing, Cyber

CLASSIFICATION: Unclassified

This paper examines current Internet attack trends in the computer networking environment and proposes an enhanced framework for system defense that is applicable to both corporate and government networks. Network defenses are typically designed, implemented, and managed at corporate computing centers and in the U.S. Department of Defense, at installation-level and regional area processing centers. Industry-wide Information Assurance best business practices and computer defensive measures are not uniformly implemented, so an enhanced security framework is necessary to assist with prioritizing and coordinating defensive efforts. The U.S. Chief Information Officer proposes that the Federal Government migrate its vast network of computer systems, through consolidation, to a more enterprise-focused architectural solution. This effort requires an expanded security framework, based on accepted network defensive principles, to reduce risks associated with emerging virtualization capabilities and scalability of cloud computing. This expanded defensive framework can assist enterprise networking and cloud computing architects to better design more secure systems.

A STRATEGIC APPROACH TO NETWORK DEFENSE: FRAMING THE CLOUD

> Agencies must focus on consolidating existing data centers, reducing the need for infrastructure growth…, and increasing their use of available cloud and shared (virtual) services.[1]
>
> —Vivek Kundra
> U.S. Chief Information Officer

The U.S. Government has robust data networks that provide rapid transport of imagery, textual information, command and control data, and routine communications to support military operations and core business needs. This information is vital in the conduct of its ongoing war and peacetime missions. Historically, America's adversaries attempt to leverage network vulnerabilities to gain strategic advantage by exploiting information about U.S. military and commercial activities, trade secrets, financial information, system architectures, and myriad other data. The U.S. is arguably the most interconnected nation on earth and it plays a hegemonic role with regards to establishing and maintaining the rules that govern the Internet. Americans embrace digital technologies and desire greater interconnection for governmental, corporate, and personal utility.

This paper examines current Internet attack trends in the computer networking environment and proposes an enhanced framework for strategic system defense that is applicable to both corporate and Federal networks. The enhanced framework addresses these issues and assists in reducing the risks associated with assessing and adopting cloud computing. Computing clouds are large data centers filled with generic processing and storage facilities, operated as a single virtual computer or multiple reconfigurable servers.[2] Previously, cloud computing was basically the outsourcing of

an organization's computing infrastructure. Emerging cloud computing technologies will subsume existing enterprise networks and encompass system defenses that are typically designed, implemented, and managed at corporate information technology (IT) and regional processing centers. Once applications are logically extended through virtualization in a cloud computing environment, they are no longer tied to a physical location. The cloud service provider can develop dispersed support and hosting facilities that allow applications to perform as needed. The system user need merely access the typically web-based application to run any desired program.

The trend for networking infrastructures and computing centers is shifting toward consolidation for cost savings. Cloud computing provides for the outsourcing of entire networking and data centers, saving physical space, infrastructure, and labor costs. The prime benefit is the reduced cost of updating corporate information systems and infrastructures, which is transferred to the cloud computing provider.[3] Cloud computing is a major evolutionary leap forward in technology that virtualizes servers, infrastructures, and software as pay-for-use services. Leaders in the Federal Government, and in particular the Department of Defense (DOD), have identified the significant benefits gained by adopting cloud computing, but they have not adequately considered the risks inherent with outsourcing information technologies.

Why Cloud Computing

Vivek Kundra, U.S. Chief Information Officer (CIO), proposes the Federal Government migrate its expansive computer networks away from a distributed architecture to a consolidated enterprise cloud computing architecture. In 2010, the White House initiated the Federal Data Center Consolidation Initiative (FDCCI) and issued guidance for the Federal CIO Council to have departments inventory their data

center assets, develop consolidation plans, and integrate those plans into fiscal year 2012 budget submissions.[4] The FDCCI's goals are to: promote IT solutions that reduce energy and physical space usage; reduce the cost of data center hardware, software, and operations; increase IT security posture; and shift investment to efficient computing platforms that will lead to closing 800 data centers by 2015.[5] Based upon this proposed migration, an expanded defensive framework that includes the evolving cloud computing environment, built on accepted network security principles, is critically needed. This expanded defensive framework would assist enterprise networking and cloud computing architects to better design more secure communication systems.

Cloud service models describe IT design capabilities and levels of autonomy for customers. There are three accepted industry-wide cloud service models: Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS).[6] The initial capabilities that are migrating to cloud environments are electronic mail, content archiving, and vendor provided SaaS applications. All benefit from consolidation into a virtualized cloud environment because these capabilities tend to require low processing cycles on servers.

However, there is a migration paradox with some IT capabilities. Computationally high cycle rate applications, transactional databases, and financial systems, due to regulatory requirements, are ill-suited for cloud computing. With SaaS and PaaS, the customer cannot change the cloud environment. SaaS is the most restrictive and only provides vendor delivered applications that customers can use, while PaaS allows customers to create programs using provided development tools and coding languages.[7] IaaS allows customers to operate on-demand virtual machines, load

software, control firewalls, and adjust networking components.[8] Within this model, the cloud provider will manage their physical servers; however, customers that employ their own applications in PaaS and virtual servers in IaaS will be required to maintain and secure their own applications and virtual systems, respectively. The implication is that if an organization is already lacking in their security regime, then migrating to a cloud environment will not necessarily improve the overall security posture. Lastly, government and private sector budgets are shrinking, so IT and data security investments must accomplish more with less resources. Adopting cloud computing is no panacea but may assist in accomplishing these cost saving efforts.

Cyberspace, Information Assurance (IA), and Network Defense

Cyberspace is defined in Joint Publication 1-02 as "a global domain within the information environment consisting of the interdependent network of IT infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[9] Cyberspace is a contested domain, and the nation is "vulnerable to threats posed in cyberspace, while at the same time, dependent upon unfettered access."[10]

Internet proliferation is exponentially expanding across the globe bringing diverse people into an ever more interconnected cyber world. Based on Moore's Law, cyberspace should continue to expand, doubling every two years with no upper limit in sight. The combination of easily affordable IT and rapidly expanding interconnectivity are changing the way that government, business, and individuals think, interact, and work.[11] The networks provide the means to rapidly share information making cyberspace, in a broader sense, a global commons for electronic information in the same fashion that the high seas are a global commons for maritime trade.[12] Thus,

cyberspace is truly international and available for all to use. It is a shared resource that is loosely governed, routinely navigated via myriad uncharted routes, and, of increasing concern, often not well-secured.

With cyberspace quickly becoming a new global commons and rapidly growing under volatile, uncertain, complex and ambiguous conditions, governments, businesses, and individuals need to balance the information triad of confidentiality, availability, and integrity as part of a stable information security model. *Confidentiality* is the term used to describe preventing the disclosure of information to unauthorized individuals or systems. In information security, *integrity* means that data cannot be modified undetectably.[13] For any information system to serve its purpose, data must be *available* when it is needed. This model is known as the *CIA Triad* of IA, as shown in Figure 1.

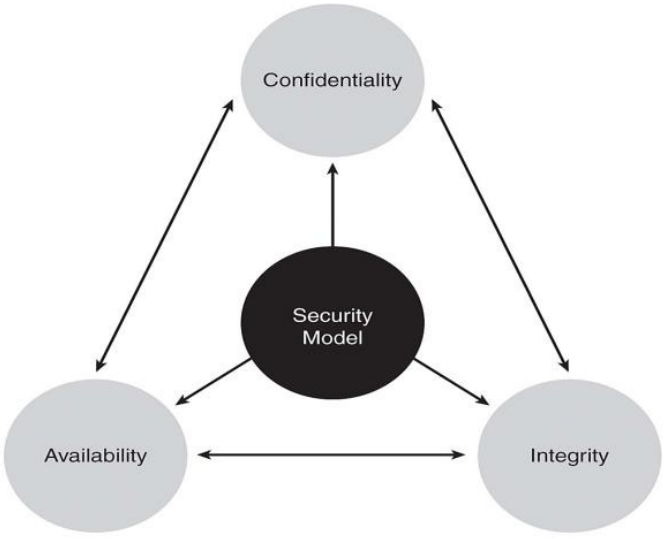

Figure 1. CIA Triad[14]

Security models are of critical importance in today's interconnected world, because information is routinely stored in large data centers that provide continuous access at the speed of electronic transfer. At the basic architectural level, there are systems hardware, software, and communications that must be protected. In this

security model, confidentiality, integrity, and availability are often at the extremes of the triad and tradeoffs can potentially frustrate each other, so system designers must endeavor to find equilibrium among them. Favoring any one design direction over the other(s) may compromise the integrity of the other triad pillars. This means for computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must function well and be in balance within this security model.[15]

DOD Directive 8500.01E establishes roles and responsibilities, procedures, and processes while defining the components of the CIA Triad.[16] IA is the means by which IT managers attempt to protect, maintain, and provide IT security to their organization through the training, testing, and constant monitoring of controls implemented to secure an information resource.[17] IA offers measures that defend information by ensuring availability, integrity, authentication, confidentiality, and non-repudiation, while providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.[18] With today's networks, these IA defensive measures are implemented through a *Defense-in-Depth* framework of layered security that extends from the network to the endpoint computer. These need to be expanded further to reduce risk more effectively in emerging cloud computing environments, while addressing Internet attack vectors and vulnerabilities that threaten the global information commons.

Framing the Strategic Environment of Cyberspace

Attacks in cyberspace are fast and can simultaneously target a precise or a broad spectrum of systems. Attackers are often anonymous with few concerns about attribution. The instantaneous nature and the ability to attack the entire domain

simultaneously are characteristics that make cyberspace potentially a more dangerous and vulnerable environment for the unprepared than traditional warfighting domains.[19]

The U.S. Government identified the IT sector as an area of the nation's critical infrastructure and aligned its protection through the Department of Homeland Security (DHS) in 2009.[20] According to the National Academy of Engineering in Washington, D.C., cyber systems are the weakest link in our national security.[21] An example is System Control and Data Acquisition (SCADA) systems that manage critical utilities, such as electrical grids, water, sewer, and gas systems for regions, states, and local communities. Older SCADA systems incorporated limited security because they operated on closed communication systems, but most modern SCADA systems use the Internet to pass control information.[22] SCADA systems are potentially exposed to asymmetrical attack from our adversaries, which could undermine U.S. capabilities and its networks.[23] On average, it is estimated that 24 hours of SCADA down time from a major attack would cost $6.3 million with costs being the highest in the oil and gas sectors.[24] SCADA attacks are serious because direct control of operational systems could create the potential for large scale power outages or man-made environmental disasters.[25] SCADA systems are vulnerable, so greater efforts are required to design and place SCADA systems in more secure architectures.

Over the years, various commissions have examined cyber security and focused their efforts on SCADA systems, communications, financial networks, and other infrastructures. Reports conclude U.S. critical infrastructures are increasingly dependent on information and communication systems, and that dependence is a source of rising vulnerabilities.[26] In 2003, Presidential Executive Order 13286 required the U.S. protect

against “disruption of the operation of information systems for critical infrastructure and help to protect the people, economy, essential human and government services, and national security of the U.S., and to ensure that any disruptions that occur are infrequent, of minimal duration, and manageable, and cause the least damage possible.”[27] IT is crucial to every aspect of modern life, and a serious attack could cripple systems for emergency services, military use, health care delivery, and electrical power generation.[28] Thus, a cyber campaign would almost certainly be directed against the country’s critical national infrastructure that would cross boundaries between government and the private sector, and, if sophisticated and coordinated, would have both immediate impact and delayed consequences.[29]

According to the U.S. Computer Emergency Readiness Team (US-CERT), cyber threats against the U.S. are broadly categorized into five potentially overlapping groups, consisting of: national governments, terrorists, industrial spies and organized crime groups, hacktivists, and hackers.[30] Any of these threat groups can have significant impacts against U.S. communication and SCADA systems, and consequently our infrastructure. Of greatest concern are national-level cyber warfare programs that pose threats along the entire spectrum of objectives that might harm U.S. interests.[31] Among the array of cyber threats, only foreign government-sponsored programs are developing capabilities with the future prospect of causing widespread, long-duration damage to U.S. critical infrastructures.[32]

Traditional terrorist adversaries of the U.S., despite their intentions to damage U.S. interests, are less developed in their computer network capabilities and propensity to pursue cyber means than are other types of adversaries.[33] They are likely, therefore,

to pose only a limited cyber threat. The U.S. should anticipate that more substantial cyber threats are possible in the future as a more technically competent generation enters the ranks.[34] International corporate spies and organized crime organizations with profit-based goals pose a medium-level threat to the U.S. through their ability to conduct industrial espionage and large-scale monetary theft, as well as their ability to hire or develop hacker talent.[35] According to the US-CERT, hacktivists form a small, foreign population of politically active hackers that includes individuals and groups with anti-U.S. motives. Motivated by propaganda and money rather than damage to critical infrastructures, hacktivists seek to achieve notoriety for their political cause.[36] Although the most numerous and highly publicized cyber intrusions are ascribed to individual hacking hobbyists, they pose a negligible threat of widespread, long-duration damage to national-level infrastructures.[37] The large majority of hackers do not have the motive or requisite tradecraft to threaten difficult targets such as critical U.S. networks. Nevertheless, the large worldwide population of hackers poses a relatively high threat of an isolated or brief disruption causing serious damage, including extensive property damage and loss of life. As the hacker population grows, so does the likelihood of a highly skilled and malicious hacker attempting and succeeding in such an attack.[38]

According to Symantec, the U.S. was the top-ranked country for malicious activity, accounting for 23 percent of all attacks, as shown in Table 1.[39] It is apparent from this report that malicious activity is prevalent in the developed and rapidly developing nations of the world, and that attacks can cross all traditional boundaries regardless of governmental, commercial, economic, and individual affiliation. The

Internet is a permissive commons and as a consequence, so is its associated malicious actors, activities, and threats.

Rank	Country/Region	Percentage	Malicious Code Rank	Spam Zombies Rank	Phishing Website Hosts Rank	Bots Rank	Attack Origin Rank
1	United States	23%	1	3	1	2	1
2	Brazil	6%	6	2	10	3	3
3	India	6%	2	1	30	20	8
4	Germany	5%	11	5	3	4	7
5	China	4%	3	28	7	6	2
6	United Kingdom	4%	4	7	4	9	4
7	Taiwan	4%	23	12	15	1	9
8	Italy	4%	21	11	11	5	6
9	Russia	3%	15	9	8	16	5
10	Canada	3%	8	41	2	17	12

Table 1. Malicious Activity by Country and Region[40]

While non-state sponsored computer network exploitation poses a serious risk to U.S. national security, those exploits are less troubling when compared to a nation-state threat, such as that of China, which seeks to go beyond cyber espionage in order to achieve military effects in future cyberspace.[41] Typically, specific information about attacks against U.S. Government networks, attribution, and successful penetration is classified, so only representative open-source information is examined, such as that in Table 1. However, from the discussion about SCADA attacks, one can surmise that military effects, such as a shutdown of regional power generation systems and distribution networks to data theft, are plausible examples across a broad range of realistic possibilities. As cyber technology becomes increasingly integrated into all facets of civilian and military life, U.S. national security planners see its pervasiveness as both a target and a weapon, similarly to other capabilities and forces; so from this perspective, it is the one critical component upon which many modern societies depend, a dependence that is not lost on potential enemies.[42]

Why Network Defense Matters

Dennis Blair, former Director of National Intelligence, stated that "the cyber criminal sector, in particular, has displayed remarkable technical innovation with an agility presently exceeding the response capability of network defenders…Criminals are collaborating globally and exchanging tools and expertise to circumvent defensive efforts, which makes it increasingly difficult for network defenders and law enforcement to detect and disrupt malicious activities."[43] Internet-related economic losses reached $42 billion in the U.S. and $140 billion worldwide in 2008, while globally, companies could have lost over $1 trillion worth of intellectual property due to data theft.[44] Stolen trade secrets, proprietary research and development information, lost royalties, patent and copyright infringement, and financial information comprise the growing magnitude of data loss due to Internet-related theft. Thus, a brief examination of defensive capabilities to protect U.S. cyberspace is necessary. Figure 2 presents the classic security "onion" diagram employed in IT environments. It focuses on traditional physical, procedural, technical and personnel security that impact on the core IT components of data, applications, hosts, and networks.

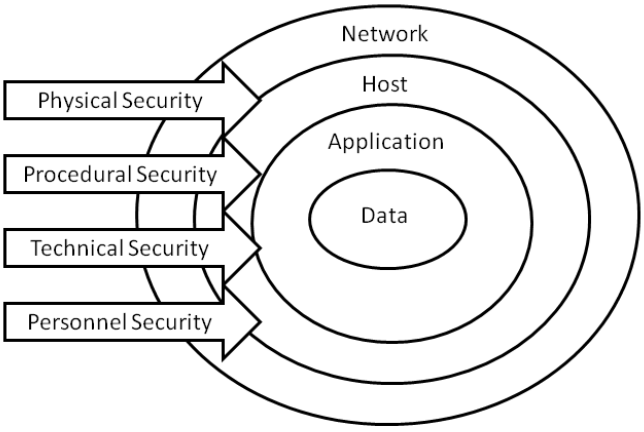

Figure 2. Classic Security "Onion"

Over time, more robust defensive constructs evolved to better protect information, servers, systems, and transport communications. As newer capabilities are brought to the marketplace, defensive technologies adjust and adapt to the changing environment. Previously, technology companies sped new capabilities into the marketplace and security measures followed as an afterthought. This circumstance frequently left significant security gaps in organizational cyber environments. In today's environment, security is a basic design consideration when products and systems are proposed. Information technologies that lack defensible capabilities are doomed to fail the user, company, or government employing them. A more modern information security construct is presented in Figure 3. While this security construct is not all inclusive, it is representative of the defense-in-depth concept that will continue to evolve as new capabilities and mediums enter cyberspace.[45]

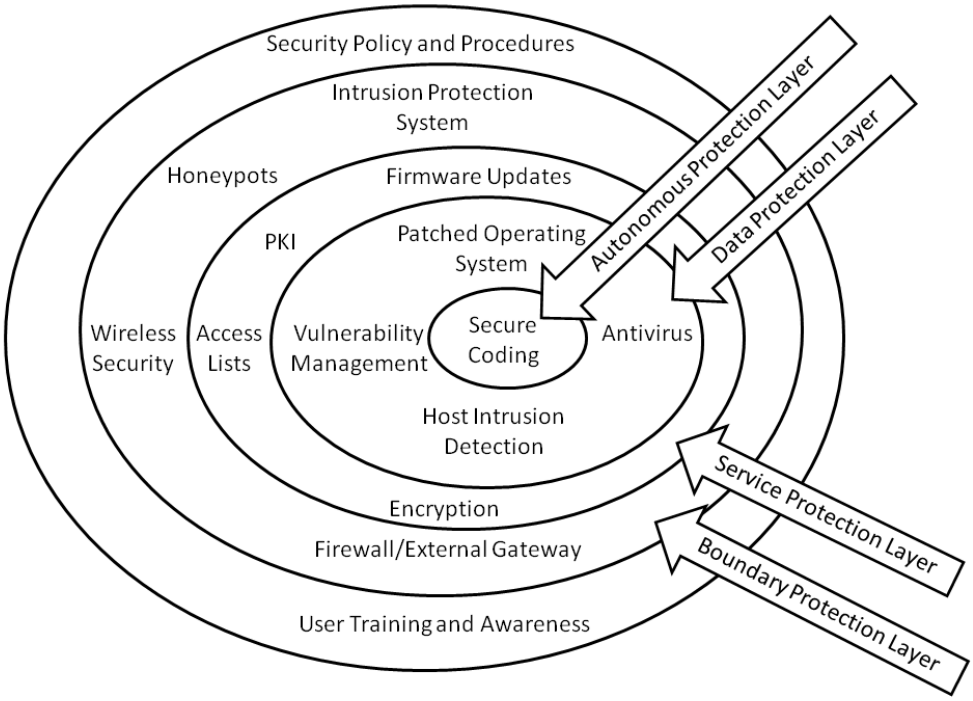

Figure 3. Modern Layered Defense Adapted from DHS Cyber Defense Strategy[46]

McAfee, a trusted leader in the computer security industry, surveyed over 1,000 businesses. Their research has national security implications which indicate that substantial amounts of vital digital information, such as intellectual property and sensitive customer data, is being transferred between companies and continents and subsequently lost.[47] The report concludes that companies lost on average $4.6 million worth of intellectual property in 2008.[48] It is difficult to evaluate the total financial losses to businesses because companies are reluctant to accurately report the figures due to concerns over losing consumer confidence. It costs an average of $600,000 per firm to respond to each security breach concerning the loss of vital information, which reflects just the reported costs of cleanup such as legal fees, victim notifications, but not infrastructure costs associated with prevention and detection.[49] The research further revealed that respondents worried more about their company's reputation due to public relations damage and information leakage than about the financial impact.[50]

An assumption is that migrating an organization's systems and capabilities to a cloud computing environment does not forgo the necessity to appreciate the changing nature of the cyber threat; nor does it allow for the abdication of security maintenance responsibilities by the data owner. Cloud computing does not change the available defensive means available to security specialists. However, protection of the physical computers becomes paramount in a cloud computing environment. If the physical server is compromised, then the hosted virtual computers will likely all be compromised as well. The reverse is not necessarily the case. This places a heightened focus on the provider's abilities to protect the physical servers, the center of gravity, in a cloud computing environment. Statistics indicate that one-third of breaches result from lost or

stolen laptop computers and from employees accidentally exposing data on the Internet with nearly 16 percent due to insider theft.[51] When a user logs out from cloud computing services, the browser can be set to flush automatically, leaving nothing on the desktop to be lost or stolen. Therefore, security concerns with cloud computing are more a cultural issue associated with outsourcing than on any proven design weakness.[52]

Cloud Computing Defense Examination

Due to the implications to broad U.S. interests, a cyber security framework for cloud computing should be developed to actively shape protection efforts for U.S. cyber infrastructure, communication systems, and commercial, financial, and especially military networks from a broad range of crippling attacks and exploitive threats. Failure to protect U.S. governmental, military, and commercial networks could lead to the loss of intellectual property, trade secrets, and more. The compromise of these crucial networks would create chaos in banking, governmental, and military systems.

Traditionally, a defense-in-depth approach is applied to securing physical IT environments. This defensive approach may be less than adequate for cloud computing environments because systems are virtual and potentially mobile. Additionally, the instantaneous nature and the ability to attack the entire cyber domain make it potentially vulnerable.[53] Physical borders are important because cloud providers select their sites based on economic, connectivity, power availability, and security criteria, but they have to make special arrangements among countries where data-movement restrictions apply.[54] Securing present day networking architectures with physical infrastructure presents known system environments to defend. However, cloud computing environments require additional risk consideration because the capabilities, data, and

software are virtualized, while the physical infrastructure is out-sourced and may reside outside the trusted governance laws of a country.

A growing number of people believe cloud computing presents a paradigm shift in computing, on a par with the development of mainframes, personal computing, client-server computing and the Internet.[55] However, system owners are generally risk adverse, so adopting cloud computing as a solution requires a comprehensive defensive framework to ensure security. While cloud computing services are currently being used, experts cite security, interoperability, and portability as major barriers to further adoption.[56] Conversely, senior IT leader expectation is for enabling cost savings and an increased ability to quickly create and deploy enterprise applications.[57] This is where current policy and subsequent security framework is lacking. Working with other agencies, industry, academia, and standards development organizations to correct this circumstance, the National Institute of Standards and Technology is leading the development of standards for security, interoperability, and portability for the U.S. CIO.[58] The expectation is that well-defined standards will shorten the adoption cycle, enabling cost savings and an increased ability to quickly create and deploy enterprise applications.

Additionally, a government-wide risk and authorization program for cloud computing will allow agencies to use the authorization by another agency with the aim to drive to a set of common services across the government supported by a community, rather than an agency-specific risk model.[59] This effort is important because it will reduce the staff's burden in performance of lengthy IA certification and accreditation of applications and systems for greater cost efficiency.

Network State-of-the-Art Risk Framework

Industry-wide IA best business practices and computer defensive measures are not uniformly implemented, so a framework is necessary to assist with prioritizing and coordinating these defensive efforts. From a defense-in-depth perspective, cyber security is not just about deploying specific technologies to counter certain risks, as such; an effective security program for any organization will depend on its faithfulness and willingness to accept security as a constant constraint on all cyber activities.[60] The critical aspect for cloud computing environments is to understand what the new and inherent risks are and how the change in service delivery might be affected. Risk assessments are a key cornerstone in defining, understanding, and planning remediation efforts against specific threats, potential vulnerabilities, and architectural design flaws.[61] Thus, the establishment of an enhanced defensive framework for cloud computing environments is prudent.

According to the DHS, a defense-in-depth framework at a minimum should include the following areas:

1. Know the security risks that an organization faces,
2. Quantify and qualify risks,
3. Use key resources to mitigate security risks,
4. Define each resource's core competency and identify any overlapping areas,
5. Abide by existing or emerging security standards for specific controls, and
6. Create and customize specific controls that are unique to an organization.[62]

Understanding that a framework is a guide for assessing risk, the basic framework is a valuable starting point. In a more traditional layered defensive construct, the systems tend to be collocated in a single or relatively close proximity networking or area data

processing center, which is often managed and controlled by the system and data owner.

The challenge for incorporating more secure cloud computing is twofold. First, the owner's data and systems are often outsourced to an external cloud computing environment provider, so the owner no longer sets the environment's security policy or maintains its security posture. Second, cloud computing environments are established in multiple locations that are virtually interconnected. Its physical servers are often located in geographically inexpensive areas in terms of labor and governmental regulation.

By entering into a cloud computing environment, there are significant benefits to an organization through the reduction of its organic technical staff, which may free up capital for other uses. The downside is that the governance of the cloud environment is not transparent, so the service and data owner could unknowingly inherit higher risk for intrusion from the provider. Once an organization outsources its technical support, it is difficult to reestablish organic technical skill sets. Simply stated, it takes years to develop institutional knowledge and then be able to apply that knowledge toward technical solutions for an organization. However, cost savings is often the driving force for adopting cloud computing. The key technical benefits are scalability and flexibility that allow an organization to pay for cloud computing resources as needed. An example of scalability comes from the private sector when their cloud computing environment allowed for a rapid response as demand jumped from 25,000 to more than 250,000 users in less than a week.[63] Because of the cloud computing technology, the company was able to scale from 50 to 4,000 virtual machines in three days to support the

increased demand.[64] This capability would take significantly longer under our current construct. Lastly, if the cloud service provider provides secure services, then the users of those capabilities will be well-served. Ultimately, the adoption of cloud computing comes down to costs, technical staff capabilities, risks, and benefits. Those factors have to be weighed carefully when making the correct decision to migrate to cloud computing or not.

Enhanced State-of-the-Art Risk Framework for Cloud Computing

Due to the tendency for outsourcing of the cloud computing environment, this paper proposes to add five additional areas to the existing defense-in-depth framework. Below are the proposed areas:

1. Assess the security posture of the cloud computing environment,
2. Know the physical location of the actual cloud computing center(s),
3. Understand your service-level expectation relative to perceived risks,
4. Assess applicable governance, laws, regulations and policies, and
5. Know your tolerance for service interruption, data loss, and recovery.

With these additional framework layers, organizations will be able to better assess their information security posture. Risk assessment is a cornerstone in prudent system design. Having an accurate and well-documented architecture and complementary risk assessment empowers an organization to be more security conscious, deploy effective security countermeasures, and be equipped to understand security incidents more readily.[65] In cloud computing the service provider establishes the cloud's architecture, security posture, and provides the service delivery. However, it is incumbent on the organization as the service and data owner to fully appreciate and assess all the environmental risks.

Cloud computing environments are a new frontier with very few specific legislative standards for security or data privacy, and there is limited governance because laws lag behind the technology development.[66] In the cloud computing environment delivery of capabilities fall into three broad categories: SaaS, PaaS and IaaS. Providers herald the robustness of their systems, often claiming that cloud environments are more secure than existing enterprise environments, but the facts are that any security measure ever breached was once thought to be infallible.[67] At present, security is imbued in the cloud computing environment, but the level of defensive measures and their implementation may vary significantly between providers.

Applicability for U.S. Federal Enterprise Environments

Arguably, the DOD operates one of the larger and more robust enterprise computing environments in the world. The Secretary of Defense, Robert Gates, in his January 2009 testimony before congress stated, "With cheap technology and minimal investment, current and potential adversaries operating in cyberspace can inflict serious damage to DOD's vast information grid – a system that encompasses more than 15,000 local, regional, and wide-area networks, and approximately 7 million IT devices."[68] Although the DOD's network structure is linked, the military services and agencies typically operate distinct domains, so it would require a vast financial and labor effort to migrate to a cloud computing environment. The consolidation effort will also drive the military services to examine IT investments from a Title 10 perspective, which may limit their autonomy with regard to their mandate to man, equip, and outfit their forces. This migration will likely occur incrementally over the next 5-10 years and may allow for the recapitalization of hundreds of millions of dollars in network operating funds. As shown in Table 2, the DOD currently spends over $36.3 billion annually for IT, according to the

IT Dashboard.[69] This dashboard provides the public with online details of U.S. Federal Government IT investments based on Federal agencies' monthly reports to the U.S. Office of Management and Budget.[70]

Bureau	Total FY2011 Spending (Billions)	No. of Total Investments
Department of the Army	$7.30	256
Department of the Air Force	$6.80	651
Department of the Navy	$7.60	789
Department of Defense Agencies	$14.60	536
Department of Defense (Total)	**$36.30**	**2232**

Table 2. U.S. DOD IT Portfolio Budget for FY2011[71]

The Federal Government, as part of a broader IT transformation, needs to fundamentally shift its mindset from building custom systems to adopting light technologies and shared solutions.[72] This is necessitated because departments and agencies typically build systems that duplicate capabilities and lack integration within the government, causing unnecessary IT redundancies and increased costs. An example is the explosion in the number of Federal data centers from 432 in 1998 to 2,094 in 2010 that highlights this ongoing IT expansion.[73] With a subjective examination of the DOD IT expenditures juxtaposed across the Federal Government above, one can sense the potential cost savings in the billions of dollars by eliminating IT redundancies, consolidating server farms and data centers into cloud computing environments, and the reduction of technical staff.

Information services should enable the departments and agencies to better serve the American people. Despite spending more than $600 billion on IT over the past decade, the Federal Government has achieved little in terms of the productivity improvements that private industry has realized from IT.[74] This reflects the growing dependency on information systems by Federal employees to accomplish their daily

work. Unless checked by a transition to cloud computing, this IT growth trend will persist and expand. However, the National Security Agency, like other Federal agencies, is trimming its spending on IA from $915 million in 2010 to $902 million in 2011.[75] It is likely this trend of reducing expenditures for IT security will continue across the Federal Government as budgets tighten.

IT projects often run over budget, fall behind schedule, or fail to deliver promised functionality because a project designer's approach simply aims to deliver full functionality in a few years, rather than modularizing projects into more manageable chunks and demanding new functionality every few quarters.[76] This circumstance is complicated because of the reliance on proprietary application and system designs when cloud computing solutions might suffice. This amounts to a change in mindset as well as an adjustment to the key functions of management and staff of the IT efforts. If cloud computing is the next generation environment, then substantial training of technical staff will be required. Although there will likely be reductions in some technical staffing areas, such as server system administrators, network maintenance and monitoring personnel, and router and gateway administrators, there will likely be increases in application and data developers. Undoubtedly, these increases will be less than offsetting, so organizations can anticipate some overall reduction in technical staff. Once gone, that knowledge will be difficult to replace. Lastly, technical staff often helps to translate executive and senior leader ideas into automation realities, so the net loss of technical staff may impede some automation understanding because of the presumed reduction of computer savvy staff.

Future IT Security Challenges

The 2010 Joint Operating Environment (JOE) indicates that "the globe-spanning range of cyberspace and its disregard for national borders challenge our legal system and complicate our ability to deter threats and respond to contingencies."[77] This recognizes that information shared across networks continues to increase while concurrently reshaping our society. The concept of having borders in cyberspace loosely exists, but this is reflected as physical network domain borders for enclaves or possibly as publically and privately facing world wide web pages as well. Traditionally, laws in many countries recognize sovereign borders, but this Westphalian concept is difficult to enforce in cyberspace. An example is the *Safe Harbor* agreement between the U.S. Department of Commerce and the European Union that attempts to bridge the gaps between the numerous privacy laws and regulations over the cross-border flow of personal information.[78] It allows companies to share information, while avoiding interruptions in their business dealings or facing prosecution by authorities under European privacy laws.[79] The problem with this type of agreement is enforcement. Thus in nine years, the U.S. Federal Trade Commission obtained consent decrees that prohibited only six U.S. companies from misrepresenting privacy and security compliance but never imposed any penalties.[80] Therefore, data sharing on the Internet permeates sovereign borders, but laws governing commerce data are specific to each country. This circumstance poses a growing challenge for implementation of cloud computing environments that may potentially handle regulated and other sensitive data between multiple countries.

Future security threats will challenge lawmakers, strategists, businessmen, and technologists to develop new approaches to operating in cyberspace. According to the

JOE, there are no protected zones or rear areas in cyberspace because all are equally vulnerable.[81] As airpower transformed the World War II battlefield environment, cyberspace permeates physical barriers that shield a nation from attacks on its commerce and communication.[82] Moreover, there is some expectation that future wars will include cyberspace as a prime venue for frontline and asymmetric operations and conflict resolution. This places information managers in a reactive position to develop countermeasures for new attacks. Once feasible defenses are established, attackers will continue to devise new methods to gain access. The challenge for defenders is that there are thousands of flaws an attacker can exploit, but the attacker only needs to find one that works to succeed.

The U.S. Government Accountability Office's (GAO) Director of Information Security Issues, Gregory Wilshusen, testified that "the four most prevalent types of incidents reported to the US-CERT during fiscal year 2009 were: (1) malicious code comprising 23 percent; (2) improper usage, 20 percent; (3) unauthorized access, 16 percent; and (4) unconfirmed incidents under investigation, 36 percent."[83] He also stated that "GAO and agency inspectors general reviews continue to highlight deficiencies in the implementation of security policies and procedures at Federal agencies."[84] The predictions seem rather clear that sophisticated attacks will continue to target emerging capabilities in cyberspace, while the trends continue regarding the lack of compliance on the part of governmental agencies to address security threats.

Conclusion

This research examined the challenges associated with providing network defense in the current enterprise environment and recognizes that consolidation of area processing and networking centers into cloud computing environments is the likely

future migration path. The primary reasons for adopting a cloud computing environment are rapid scalability and flexibility with SaaS, PaaS, and IaaS. There is a perception that migration to the cloud computing environment will also yield cost savings through reduced physical infrastructure and technical staff. While the reality of reduced physical infrastructure will occur, it is not clear that the technical staff will be significantly reduced because virtualized servers still need to be maintained. Additionally, this paper proposed an enhanced defensive framework to better assess the risks of cloud computing. While the existing framework is still valuable, the added assessment areas address and capture the dynamic nature of the cloud computing environment and afford the system owner improved attack risk mitigation through a more complete assessment of the environment.

The JOE predicts that network connectivity will grow by 50% a year, providing about 100,000 times more bandwidth in 2030 than today; and computers will run one million times faster, so a home computer would be capable of downloading the entire Library of Congress (roughly 16 terabytes of data) in 128 seconds.[85] With these predictions in mind, it is apparent that security challenges and attack sophistication will increase proportionally. The greatest concern for government and businesses is to be lulled into a false sense of security by adoption of cloud computing environments. The benefits are equally apparent, but the consolidation of multiple virtual machines into an outsourced cloud computing environment incurs some risk. If the physical server fails, then the numerous virtual machines will go silent. Equally, if the physical server is compromised, then the hosted virtual computers will likely be as well. Ultimately, it boils down to data owner risk, expectations, and tolerance of not controlling their systems.

With commitment, careful planning, and systematic implementation the defense needs to incorporate cyberspace's virtual world, if there is any chance of limiting damage in the real world.[86] The defense of virtual computers is more akin to holding atmosphere in your hand or cyberspace as the case may be. Clausewitz stated, "The defender is at greatest disadvantage when compelled to protect a wide area against multiple axes of advance. In this instance, the attacker using surprise may throw his full strength at any one point."[87] Conclusively, the network defense employs substantially more means to preserve security in computing environments, so the attacker may actually have the initiative and an asymmetric advantage in cyberspace. However, well-designed cloud computing environments may change the balance back in favor of the defense, while reducing costs and improving service.

Endnotes

[1] U.S. Chief Information Officer Vivek Kundra, *25 Point Implementation Plan to Reform Federal Information Technology Management* (Washington, DC: The White House, December 9, 2010), 5.

[2] Clive Davidson, "Cloud Control," *Risk* 23, no. 10 (October 2010) in ProQuest (accessed November 22, 2010): 70.

[3] Ibid., 71.

[4] U.S. Chief Information Officer, *25 Point Implementation Plan to Reform Federal Information Technology Management*, 5.

[5] Ibid., 5.

[6] Mike Gray, "Cloud Computing: Demystifying IaaS, PaaS, and SaaS," *ZDNET*, October, 21, 2010, http://www.zdnet.com/news/cloud-computing-demystifying-iaas-paas-and-saas/477238 (accessed April 19, 2011).

[7] U.S. Department of Commerce, National Institute of Standards and Technology, *The NIST Definition of Cloud Computing (Draft)*, Special Publication 800-145 (Draft), (Washington, DC: U.S. Department of Commerce, January 2011), 2.

[8] Gray, "Cloud Computing: Demystifying IaaS, PaaS, and SaaS".

[9] U.S. Department of the Defense, *Dictionary of Military and Associated Terms*, Joint Publication 1-02, (Washington, DC: U.S. Department of the Defense, April 12, 2001 amended through September 30, 2010), 126.

[10] William T. Lord, "Cyberspace Operations: Air Force Space Command Takes the Lead," *High Frontier* 5, no. 3 (May 2009): 3.

[11] *Intel*, "Moore's Law," (Santa Clara, CA: Intel Corporation, 2010) http://www.intel.com/technology/mooreslaw/ (accessed November 19, 2010).

[12] Arthur K. Cebrowski, "Transformation and the Changing Character of War?," *Transformation Trends*, June 17, 2004, http://www.oft.osd.mil/library/library_files/trends_ 370 _ Transformation%20Trends-17%20June%202004%20Issue.pdf (accessed January 5, 2011).

[13] Chad Perrin, "The CIA Triad," (Louisville, KY: TechRepublic, June 30, 2008) http://www.techrepublic.com/blog/security/the-cia-triad/488 (accessed January 23, 2011).

[14] *Cisco Learning Network*, "What is the CIA Triad," https://learningnetwork.cisco.com/message/59995 (accessed November 19, 2010).

[15] Perrin, "The CIA Triad".

[16] U.S. Department of the Defense, *Information Assurance*, DOD Directive 8500.01E, (Washington, DC: U.S. Department of the Army, October 24, 2002, Certified Current April 23, 2007), 4.

[17] U.S. Department of the Army, *Information Assurance*, Army Regulation 25-2, (Washington, DC: U.S. Department of the Army, March 23, 2009), 1.

[18] U.S. Department of the Defense, *Dictionary of Military and Associated Terms*, Joint Publication 1-02, 175.

[19] David M. Hollis, "USCYBERCOM: The Need for a Combatant Command versus a Subunified Command," *Joint Forces Quarterly*, no. 58 (Third Quarter 2010): 49.

[20] Jeffrey L. Caton, "Cyberspace and Cyber Operations," in *Information Operations Primer*, AY11 ed., (Carlisle, PA: U.S. Army War College, November 2010), 21.

[21] *National Academy of Engineering*, "Securing the Electricity Grid," http://www.nae.edu/Publications/Bridge/TheElectricityGrid/18868.aspx (accessed January 3, 2011).

[22] Caton, "Cyberspace and Cyber Operations," 20.

[23] *National Academy of Engineering*, "Securing the Electricity Grid".

[24] *McAfee*, "In the Crossfire: Critical Infrastructure in the Age of Cyber War" (Santa Clara, CA: McAfee, 2011), 10, http://newsroom.mcafee.com/images/10039/In%20the%20Crossfire_CIP% 20report.pdf (accessed January 26, 2011).

[25] Ibid., 9.

[26] Andrew Hildick-Smith, "Security for Critical Infrastructure SCADA Systems," *SANS Institute InfoSec Reading Room*, (Bethesda, MD: SANS Institute, February 23, 2005), 5, www.sans.org/reading_room/ whitepapers/warfare/security-critical-infrastructure-scada-systems_1644 (accessed November 19, 2010).

[27] George W. Bush, *Presidential Executive Order 13286 amending 13231 Critical Information Protection in the Information Age* (Washington, DC: The White House, February 28, 2003).

[28] Hildick-Smith, "Security for Critical Infrastructure SCADA Systems," 5.

[29] Timothy Shimeall, "Countering Cyber War," *NATO Review* 49, no. 4 (Winter 2001): 17.

[30] *U.S. Computer Emergency Readiness Team*, "Cyber Threat Source Descriptions," http://www.us-cert.gov/control_systems/csthreats.html (accessed January 3, 2011).

[31] Ibid.

[32] Ibid.

[33] Ibid.

[34] Ibid.

[35] Ibid.

[36] Ibid.

[37] Ibid.

[38] Ibid.

[39] *Symantec Intelligence Quarterly Report for July – September 2010* (Mountain View, CA: Symantec, 2010), 6, http://www.symantec.com/content/en/us/enterprise/white_papers/b-symc_intelligence_qtrly_july_to_sept_WP_21157366.en-us.pdf (accessed December 15, 2010).

[40] Ibid., 6.

[41] Brian M. Mazanec, "The Art of Cyber War," *Journal of International Security Affairs*, no. 16 (Spring 2009): 84.

[42] Timothy Shimeall, "Countering Cyber War," *NATO Review* 49, no. 4 (Winter 2001): 16.

[43] U.S. Director of National Intelligence Dennis C. Blair, *Annual Threat Assessment of the Intelligence community for the Senate Select Committee on Intelligence* (Washington, DC: U.S. Senate, February 2, 2010), 4.

[44] Ibid., 40.

[45] U.S. Department of Homeland Security, *Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies*, (Washington, DC: U.S. Department of Homeland Security, October 2009), 14.

[46] Ibid.

[47] *Unsecured Economies: Protecting Vital Information* (Santa Clara: McAfee, 2009), 3, http://resources.mcafee.com/content/NAUnsecuredEconomiesReport (accessed January 8, 2011).

[48] Ibid.

[49] Ibid., 7.

[50] Ibid.

[51] Elinor Mills, "Cloud Computing Security Forecast: Clear Skies," *CNET News*, January 27, 2009, http://news.cnet.com/8301-1009_3-10150569-83.html (accessed January 26, 2011).

[52] Ibid.

[53] Hollis, "USCYBERCOM: The Need for a Combatant Command versus a Subunified Command," 49.

[54] Davidson, "Cloud Control," 72.

[55] Ibid., 73.

[56] U.S. Chief Information Officer, *25 Point Implementation Plan to Reform Federal Information Technology Management*, 7.

[57] Ibid.

[58] Ibid.

[59] Ibid., 8.

[60] U.S. Department of Homeland Security, *Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies*, 14.

[61] Ibid., 15.

[62] Ibid.

[63] U.S. Chief Information Officer, *25 Point Implementation Plan to Reform Federal Information Technology Management*, 6.

[64] Ibid.

[65] U.S. Department of Homeland Security, *Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies*, 29.

[66] David Binning, “Top Five Cloud Computing Security Issues,” *ComputerWeekly.com*, April 2, 2009, http://www.computerweekly.com/Articles/2010/01/12/235782/Top-five-cloud-computing-security-issues.htm (accessed January 9, 2011).

[67] Ibid.

[68] U.S. Secretary of Defense Robert M. Gates, *Submitted Statement to Senate Armed Services Committee* (Washington, DC: U.S. Senate), January 27, 2009), 8.

[69] U.S. Office of Management and Budget, “IT Dashboard,” http://it.usaspending.gov/ (accessed January 27, 2011).

[70] Ibid.

[71] Ibid.

[72] U.S. Chief Information Officer, *25 Point Implementation Plan to Reform Federal Information Technology Management*, 3.

[73] Ibid.

[74] Ibid., 1.

[75] J. Nicholas Hoover, “NSA Details Information Assurance Spending,” *InformationWeek*, April 9, 2010, http://www.informationweek.com/news/government/security/showArticle.jhtml?articleID=224202447 (accessed January 27, 2011).

[76] U.S. Chief Information Officer, *25 Point Implementation Plan to Reform Federal Information Technology Management*, 1.

[77] U.S. Joint Forces Command, *Joint Operating Environment* (Norfolk, VA: U.S. Joint Forces Command, February 18, 2010), 34.

[78] U.S. Department of Commerce, *Safe Harbor Overview* (Washington, DC: U.S. Department of Commerce, 2000) http://www.export.gov/safeharbor/eg_main_018236.asp (accessed January 10, 2010).

[79] Ibid.

[80] *World Privacy Forum*, “The US Department of Commerce and International Privacy Activities: Indifference and Neglect,” November 22, 2010, http://www.worldprivacyforum.org/pdf/USDepartmentofCommerceReportfs.pdf (accessed January 10, 2011), 19.

[81] U.S. Joint Forces Command, *Joint Operating Environment*, 36.

[82] Ibid.

[83] U.S. Government Accountability Office Director, Information Security Issues Gregory C. Wilshusen, *Testimony Before the Subcommittee on Government Management, Organization, and Procurement, Committee on Oversight and Government Reform, U.S. House of Representatives* (Washington, DC: U.S. Congress), March 24, 2010), 11.

[84] Ibid., 5.

[85] U.S. Joint Forces Command, *Joint Operating Environment*, 36.

[86] Shimeall, “Countering Cyber War,” 18.

[87] Carl von Clausewitz, On War, trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1989), 364.